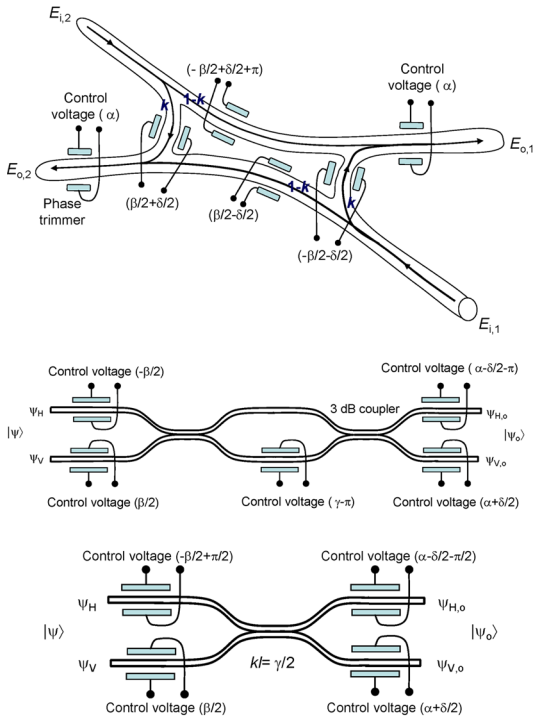
IEEE Photonics Journal
An IEEE Photonics Society Publication

On the Photonic Implementation of Universal Quantum Gates, Bell States Preparation Circuit, Quantum Relay and Quantum LDPC Encoders and Decoders

Volume 2, Number 1, February 2010

Ivan B. Djordjevic, Member, IEEE



DOI: 10.1109/JPHOT.2010.2042707
1943-0655/$26.00 ©2010 IEEE

On the Photonic Implementation of Universal Quantum Gates, Bell States Preparation Circuit, Quantum Relay and Quantum LDPC Encoders and Decoders

Ivan B. Djordjevic, *Member, IEEE*

Department of Electrical and Computer Engineering, University of Arizona, Tucson, AZ 85721 USA

DOI: 10.1109/JPHOT.2010.2042707
1943-0655/$26.00 ©2010 IEEE

Manuscript received January 10, 2010; revised February 1, 2010. First published Online February 8, 2010. Current version published February 26, 2010. This work was supported in part by the National Science Foundation under Grant IHCS-0725405. Corresponding author: I. B. Djordjevic (e-mail: ivan@ece.arizona.edu).

Abstract: We show that any family of universal quantum gates can be implemented based on a single optical hybrid/Mach–Zehnder interferometer (MZI)/directional coupler (DC) and either a highly nonlinear optical fiber or a tap coupler with an avalanche photodiode. We further show how to implement Pauli gates, which are needed in quantum error correction, using the same technology. The use of Bell states in quantum teleportation is essential. We also show how to implement the Bell states preparation circuit. To extend the transmission distance of quantum teleportation systems, the use of quantum relays is necessary. We show how to implement the quantum relay in integrated optics as well. We further study the implementation of encoders/decoders for sparse-graph quantum codes and show that the encoder/decoder for arbitrary quantum sparse-graph code can be implemented in integrated optics as well. We also study the performance of sparse-graph codes and demonstrate that entanglement-assisted sparse-graph codes from balanced incomplete block designs significantly outperform the corresponding dual-containing quantum codes. Finally, we provide several theorems that can be used in the design of entanglement-assisted (EA) quantum codes that require only one qubit to be shared between the source and the destination.

Index Terms: Quantum teleportation, quantum information processing, integrated optics devices, quantum error correction codes (QECCs), sparse-graph quantum codes, balanced incomplete block designs (BIBDs).

1. Introduction

Quantum information processing (QIP) is an exciting research area with numerous applications, including quantum key distribution (QKD), quantum teleportation, quantum computing, quantum networks, quantum lithography, and quantum memories [1]. QIP, however, relies on delicate superposition states, which are sensitive to interactions with environment, resulting in decoherence. Moreover, the quantum gates are imperfect and the use of quantum error-correction coding (QECC) is essential to enable the fault-tolerant computing and to deal with quantum errors [1]–[5]. QECC encoders/decoders are essentially based on Pauli gates. We have recently proposed encoder and decoder architectures for quantum low-density parity-check (LDPC) codes suitable for all-optical implementation, based on controlled-NOT (CNOT) and Hadamard gates only [3]. In our proposal, the Hadamard gate was based on optical hybrid (OH) technology, while the CNOT gate was based on a

directional couplers proposal from [6] and [7]. Unfortunately, the directional-coupler-based CNOT gate from [6] and [7] is essentially a probabilistic device and, as such, is not suitable for large-scale integration.

In order to perform an arbitrary quantum computation operation, a minimum number of gates, known as universal quantum gates [1], [8], [9], is needed. The most popular sets of universal quantum gates are: i) {Hadamard (H), phase (S), $\pi/8$ (T), CNOT} gates, ii) {H, S, CNOT, Toffoli (U_T)} gates, iii) the {Barenco} gate [8], and iv) the {Deutsch} gate [9]. In this paper, we show that arbitrary single-qubit gate can be implemented based on a single OH/Mach–Zehnder interferometer (MZI)/directional coupler (DC). We also show how to implement the deterministic CNOT gate based on OHs/MZIs/DCs and either highly nonlinear optical fiber (HNLF) [10] or a tap coupler with an avalanche photodiode (APD), which completes the implementation of arbitrary set of universal quantum gates in all-fiber technology.

The basic quantum circuit needed in quantum teleportation is an entanglement Einstein-Podolsky-Rosen (EPR) preparation circuit. We will show later in the paper how to implement it in all-fiber technology. To extend the transmission distance of current quantum teleportation systems, the implementation of quantum relay is of crucial importance [11]. Because this circuit is based on the EPR preparation circuit, the controlled-X gate, and the controlled-Z gate, it can also be implemented in the same technology. Another alternative technology to implement both Bell states preparation circuit and quantum relay is based on four-photon mixing (FPM), which is also known as four-wave mixing (FWM) [10], and can be implemented based on HNLFs.

Inspired by the conjecture that the best quantum error-correcting codes can be related to the best classical codes, MacKay *et al.* recently proposed [2] how to design the sparse dual-containing binary codes that can be used to construct quantum LDPC codes belonging to the class of Calderbank–Shor–Steane (CSS) codes [1]. Most of the constructions introduced in [2] are obtained by computer search. In our recent papers [3], [4], we proposed a series of structured quantum LDPC codes based on the balanced incomplete block designs (BIBDs) [12], [13]. These codes offer a number of advantages compared with other classes of quantum codes thanks to the sparseness of their quantum check matrices [2]–[4]. The most of the designs belong to the class of dual-containing CSS codes that are essentially girth-4 codes, which perform badly under sum–product algorithm (SPA) (commonly used in decoding of LDPC codes).

On the other hand, it was shown in [5] that through the use of entanglement, arbitrary classical codes can be used in correction of quantum errors and not only with girth-4 codes; this class of quantum codes is known as entanglement-assisted (EA) QECCs [5]. The number of needed preexisting entanglement qubits (also known as ebits [5]) can be determined by $e = \text{rank}(\boldsymbol{H}\boldsymbol{H}^T)$, where $\boldsymbol{H}$ is the parity-check matrix of a classical code (and $\text{rank}(.)$ is the rank of a given matrix). In this paper, we show how to design EA LDPC codes from BIBDs [12], [13] of unitary index that require only one ebit to be shared between source and destination. We provide two theorems that can be used in design of EA codes with $e = 1$. Because these codes have a girth $g = 6$, they are capable of significantly outperforming previously proposed dual-containing LDPC codes. We further propose several quite general classes of BIBDs of unitary index suitable for design of EA LDPC codes of girth 6, with the number of required ebits being one.

The paper is organized as follows. In Section 2, we describe the integrated optics implementation of universal quantum gates and Pauli gates based on a single OH/MZI/DC. The integrated optics implementation of Bell state preparation circuit and quantum relay is described in Section 3. In Section 4, we describe the implementation of encoders and decoders for sparse-graph codes in integrated optics. Section 5 is devoted to the design of EA sparse-graph codes that require only one qubit to be shared between source and destination. In the same section, we provide the comparison of EA quantum codes and dual-containing quantum codes. Finally, in Section 6, some important concluding remarks are given.

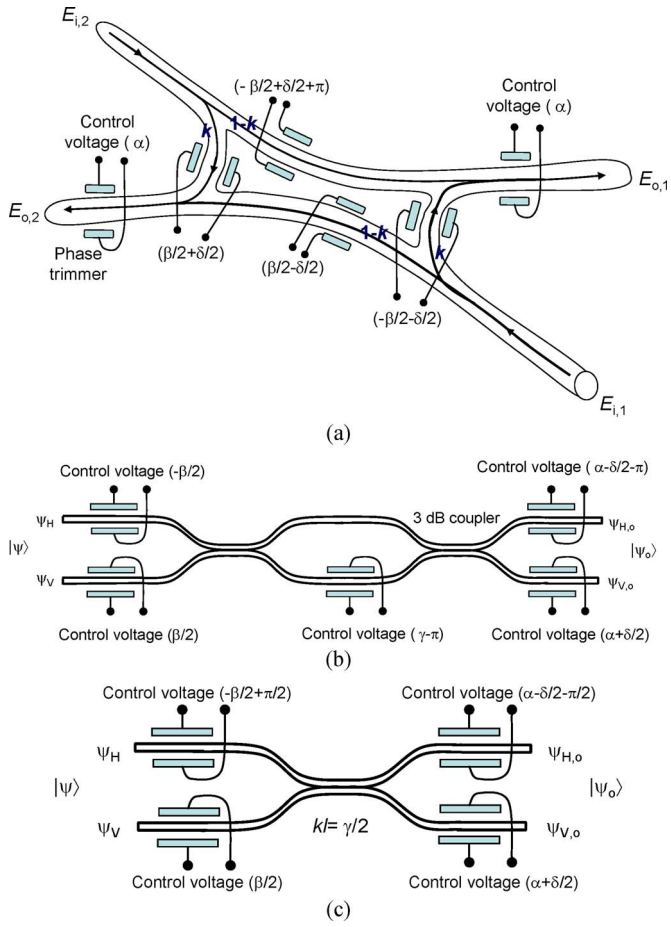


Fig. 1. Integrated optics implementation of arbitrary single-qubit quantum gate based on a single (a) OH, (b) MZI, and (c) DC (k—the coupling coefficient; l—the coupling region length).

2. Integrated Optics Implementation of Universal Quantum Gates and Pauli Gates Based on a Single OH/MZI/DC and HNLF/A Tap Coupler

In what follows, the logical "0" is represented by a horizontal (H) photon $|H\rangle = [1\ 0]^T$, and the logical "1" is represented by a vertical (V) photon $|1\rangle = [0\ 1]^T$. An arbitrary single-qubit gate can be implemented in integrated optics based on OH, as shown in Fig. 1(a). The output electrical fields $E_{o,1}$ and $E_{o,2}$ are related to the input electrical fields $E_{i,1}$ and $E_{i,2}$ by

$$\begin{aligned} E_{o,1} &= \left[\sqrt{k}e^{j(-\beta/2-\delta/2)}E_{i,1} + \sqrt{1-k}e^{j(-\beta/2+\delta/2+\pi)}E_{i,2}\right]e^{j\alpha} \\ E_{o,2} &= \left[\sqrt{1-k}e^{j(\beta/2-\delta/2)}E_{i,1} + \sqrt{k}e^{j(\beta/2+\delta/2)}E_{i,2}\right]e^{j\alpha} \end{aligned} \tag{1.1}$$

where k is the power splitting ratio, while α, β, and δ are phase shifts introduced by phase trimmers as shown in Fig. 1(a). The equation (1) can be rewritten in matrix form as

$$\begin{bmatrix} E_{o1} \\ E_{o2} \end{bmatrix} = U \begin{bmatrix} E_{i1} \\ E_{i2} \end{bmatrix}$$
$$U = \begin{bmatrix} \sqrt{k}e^{j(\alpha-\beta/2-\delta/2)} & -\sqrt{1-k}e^{j(\alpha-\beta/2+\delta/2)} \\ \sqrt{1-k}e^{j(\alpha+\beta/2-\delta/2)} & \sqrt{k}e^{j(\alpha+\beta/2+\delta/2)} \end{bmatrix}. \tag{1.2}$$

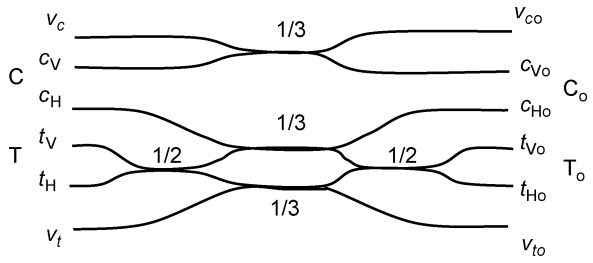


Fig. 2. Probabilistic implementation of CNOT gate in integrated optics.

By expressing the power splitting ratio as $k = \cos^2(\gamma/2)$, where angle γ is used to parameterize the power splitting ratio, the scattering matrix U from (1.2) can be written as

$$U = \begin{bmatrix} \cos\left(\frac{\gamma}{2}\right) e^{j(\alpha-\beta/2-\delta/2)} & -\sin\left(\frac{\gamma}{2}\right) e^{j(\alpha-\beta/2+\delta/2)} \\ \sin\left(\frac{\gamma}{2}\right) e^{j(\alpha+\beta/2-\delta/2)} & \cos\left(\frac{\gamma}{2}\right) e^{j(\alpha+\beta/2+\delta/2)} \end{bmatrix} \tag{2}$$

which represents the matrix representation of an arbitrary single-qubit quantum gate according to the Z-Y decomposition theorem (see [1, eq. (4.12)]).

Let the input photon (qubit) be represented by $[\psi_H, \psi_V]^T$ and the corresponding output qubit be represented by $[\psi_{H,o}, \psi_{V,o}]^T$. By employing a polarization beam splitter (PBS) at the input of OH and a polarization beam combiner (PBC) at the output of OH, by connecting the horizontal-output of PBS to the $E_{i,1}$-input and the vertical-output to the $E_{i,2}$-input, and by connecting the horizontal-input of PBC to the $E_{o,1}$-output and the vertical-input to the $E_{o,2}$-output, we can establish the following connection between output and input qubits:

$$\begin{bmatrix} \psi_{H,o} \\ \psi_{V,o} \end{bmatrix} = U \begin{bmatrix} \psi_H \\ \psi_V \end{bmatrix} \tag{3}$$

where the U-matrix is already introduced by (2). Therefore, the integrated optics circuit shown in Fig. 1(a) can indeed be used to implement arbitrary single-qubit gate. The same equation holds for the MZI-based and DC-based single-qubit quantum gates [see Fig. 1(b) and (c)]. By setting $\gamma = \delta = 0$ rad, $\alpha = \pi/4$ and $\beta = \pi/2$ rad U-gate described by (2) operates as the phase gate

$$S = \begin{bmatrix} 1 & 0 \\ 0 & j \end{bmatrix}. \tag{4}$$

By setting $\gamma = \delta = 0$ rad, $\alpha = \pi/8$ and $\beta = \pi/4$ rad, the U-gate operates as the $\pi/8$ gate

$$T = \begin{bmatrix} 1 & 0 \\ 0 & e^{j\pi/4} \end{bmatrix}. \tag{5}$$

Finally, by setting $\gamma = \pi/2$, $\alpha = \pi/2$, $\beta = 0$ rad, and $\delta = \pi$, the U-gate given by (2) operates as the Hadamard gate

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}. \tag{6}$$

To complete the implementation of set i) of universal quantum gates, the implementation of the CNOT gate is needed. The authors in [6] and [7] proposed the use of DCs to implement the CNOT gate. For the completeness of presentation, in Fig. 2, we provide a simplified version of CNOT gate proposed in [6] and [7]. We see that the control output qubit $[c_{H,o}, c_{V,o}]^T$ is related to the input control qubit $[c_H, c_V]^T$ and input target qubit $[t_H, t_V]^T$ by [6]

$$\left[c_{H,o} = (1/\sqrt{3})(\sqrt{2}v_c + c_H) \quad c_{V,o} = (1/\sqrt{3})(-c_V + t_H + t_V) \right]^T.$$

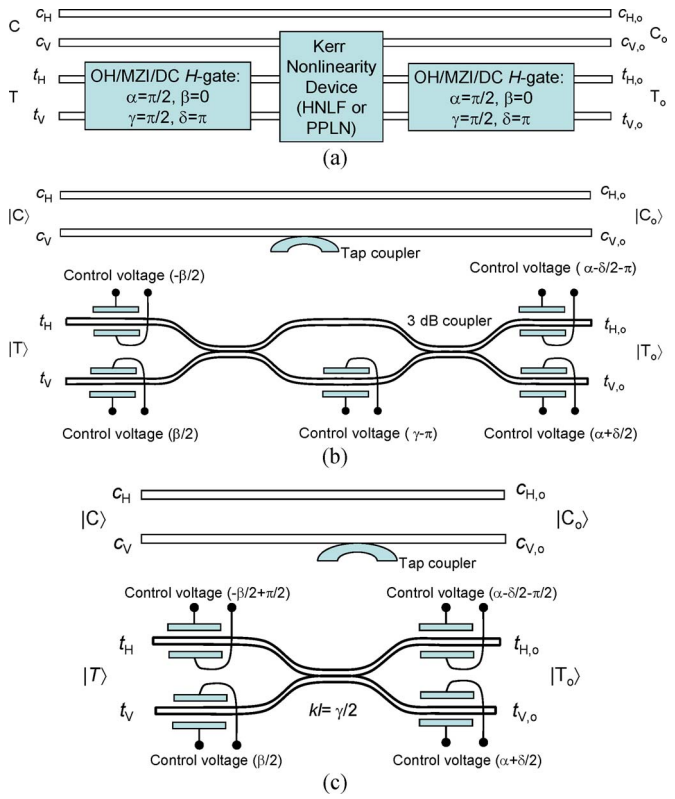


Fig. 3. Deterministic implementation of CNOT gate based on (a) OH/MZI/DC and HNLF, (b) MZI with a tap coupler and APD, and (c) DC with a tap coupler and APD. OH/MZI/DC *H*-gate: OH/MZI/DC-based Hadamard gate, PPLN: periodically poled LiNbO3.

Because the output control qubit is affected by input target qubit, the definition of CNOT-gate operation (control qubit must be unaffected by the target qubit) is violated [1]. This gate operates correctly only with probability of 1/9 and is essentially a probabilistic gate.

In Fig. 3(a), we show the deterministic implementation of CNOT gate based on OH shown in Fig. 1(a) and HNLF. By using directional coupling theory, it can be shown that output control $|C_o\rangle = [c_{H,o}c_{V,o}]^T$ and target qubits $|T_o\rangle = [t_{H,o}t_{V,o}]^T$ are related to corresponding input qubits by

$$\begin{bmatrix} c_{H,o} \\ c_{V,o} \\ t_{H,o} \\ t_{V,o} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & \cos\left(\frac{\gamma}{2}\right)e^{j(\alpha-\beta/2-\delta/2)} & -\sin\left(\frac{\gamma}{2}\right)e^{j(\alpha-\beta/2+\delta/2)} \\ 0 & 0 & \sin\left(\frac{\gamma}{2}\right)e^{j(\alpha+\beta/2-\delta/2)} & \cos\left(\frac{\gamma}{2}\right)e^{j(\alpha+\beta/2+\delta/2)} \end{bmatrix} \begin{bmatrix} c_H \\ c_V \\ t_H \\ t_V \end{bmatrix}. \tag{7}$$

The Kerr nonlinearity device in Fig. 3(a) performs the controlled-Z operation. In the absence of the control c_V-photon, the target qubit is unaffected because $H^2 = I$ (identity operator). In the presence of the control c_V-photon, thanks to the cross-phase modulation in HNLF, the target vertical photon experiences the phase shift χL, where χ is the third-order nonlinearity susceptibility coefficient, and L is the HNLF length. By selecting appropriately the fiber length, we obtain $\chi L = \pi$, and the overall action on target qubit is $HZH = X$, which corresponds to the CNOT-gate action.

The CNOT gate shown in Fig. 3(a) requires the use of fibers with very high χ, and HNLF can have different properties than optical waveguides shown in the same figure. To avoid this problem, we can use the tap coupler approach to detect the presence of the c_V-photon by an APD and perform corresponding control-operation by properly setting the α, β, γ, and δ parameters, as shown in Fig. 3(b) and (c). Notice that this step is purely classical: We detect the presence of the c_V-photon by an APD and apply the corresponding voltages. This approach is consistent with a property that

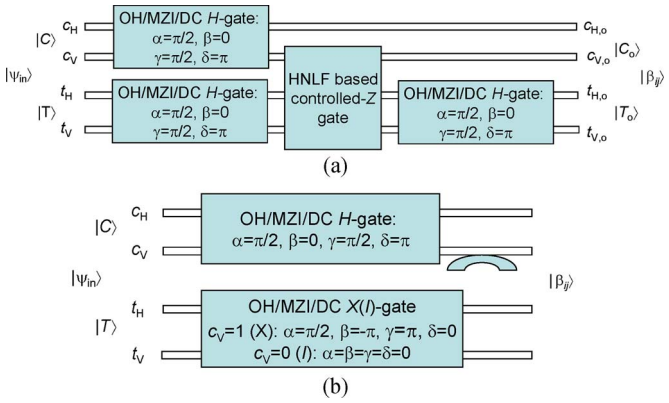


Fig. 4. Implementation of Bell states preparation circuit based on OHs/MZIs/DCs-based Hadamard gate and (a) HNLF and (b) tap coupler.

measurement commutes with a control, as shown in [1, Ex. 4.35]. In the absence of control c_V-photon, we set the parameters $\alpha = \beta = \gamma = \delta = 0$ rad, and the corresponding gate operates as an identity operator. Arbitrary c_V-photon controlled U-operations can be performed by appropriately choosing the parameters α, β, γ, and δ. For example, if we, in the presence of control c_V-photon, impose the following phase shifts $\delta = 0$ rad, $\alpha = \pi/2$ and $\beta = -\pi$ and set parameter $\gamma = \pi$, the gate described by (7) operates as the CNOT gate:

$$\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \tag{8}$$

The Toffoli gate can straightforwardly be obtained as generalization of the CNOT gate above by adding an additional control qubit. With small modifications in (7), we can easily obtain the Barenco gate, while the Deutsch gate can be obtained by employing three control qubits, instead of one, used in (7).

In the rest of this section, we describe the implementation of Pauli gates X, Y, and Z in integrated optics based on a single OH/MZI/DC. By using the U-gate shown in Fig. 1 and by appropriately setting the phase shifts α, β, γ, and δ, we can obtain the corresponding Pauli gates. The Y-gate is obtained by setting $\gamma = \pi$, $\beta = \delta = 0$ rad and $\alpha = \pi/2$

$$Y = \begin{bmatrix} 0 & -j \\ j & 0 \end{bmatrix}. \tag{9}$$

The Z-gate is obtained by setting $\gamma = \delta = 0$ rad, $\alpha = \pi/2$, and $\beta = \pi$

$$Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{10}$$

The X-gate is obtained by setting $\gamma = \pi$, $\delta = 0$ rad, $\alpha = \pi/2$, and $\beta = -\pi$:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}. \tag{11}$$

3. Integrated Optics Implementation of Bell States Preparation Circuit and Quantum Relay

We further describe the implementation of the EPR pairs (Bell states) preparation circuit based on OH/MZI/DC, which is shown in Fig. 4. In Fig. 4(a), the implementation based on HNLF is shown. The upper OH/MZI/CD circuit operates as a Hadamard gate, while the rest of the circuit operates as

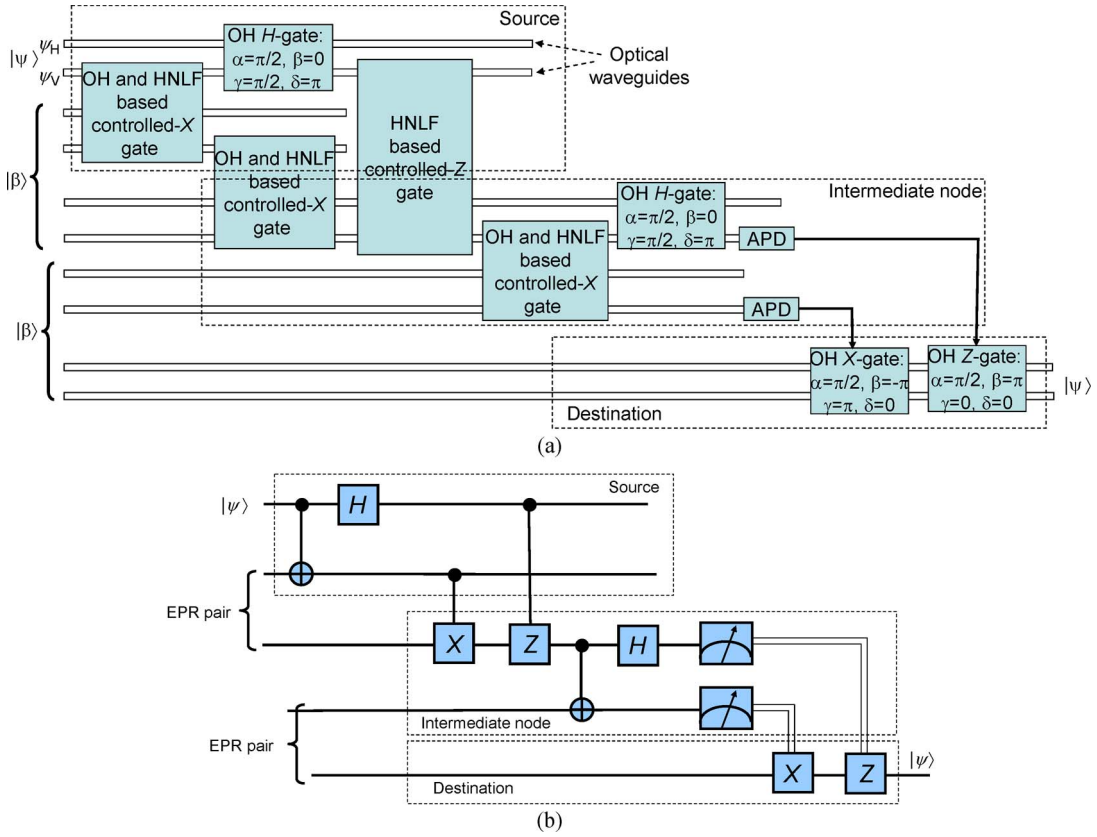


Fig. 5. (a) Integrated optics implementation of quantum relay. (b) Equivalent circuit.

a CNOT gate, as already explained in the description of Fig. 3(a). In Fig. 4(b), the implementation based on a tap coupler and an APD is shown. The upper OH/MZI/DC circuit operates as a Hadamard gate, and the lower one operates either as either an identity gate (*I* gate, by setting the phase shifts $\alpha = \beta = \gamma = \delta = 0$) or an *X* gate $(\alpha = \pi/2, \beta = -\pi, \gamma = \pi, \delta = 0)$, depending on the presence $(c_V = 1)$ or absence $(c_V = 0)$ of a vertical control photon. By using the quantum-mechanical description provided in [1], it can be shown that the output quantum state $|\beta_{ij}\rangle$ is related to the input state $|\psi_{in}\rangle$ by

$$|\beta_{ij}\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{bmatrix}$$

$$|\psi_{in}\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} c_H t_H + c_V t_V \\ c_H t_V + c_V t_V \\ c_V t_H - c_V t_V \\ c_H t_H - c_V t_H \end{bmatrix}. \tag{12}$$

For example, by setting $c_H = t_H = 1$ and $c_V = t_V = 0$, we obtain the Bell state

$$|\beta_{00}\rangle = [1 \quad 0 \quad 0 \quad 1]^T/\sqrt{2} = (|00\rangle + |11\rangle)/\sqrt{2}.$$

In Fig. 5, we describe how to implement the quantum relay based on the EPR pairs preparation circuit (shown in Fig. 4), and the Hadamard, controlled-*X*, and controlled-*Z* gates described

above. We employ the principle of deferred measurement and perform corresponding measurements only in the last intermediate node, which is a key difference with various quantum relay architectures described in [11]. The measurements circuits in Fig. 5 represent APDs, which are used to detect the presence of c_V-photons in corresponding control qubits. The detection of c_V-photons triggers the application of required control voltages on phase trimmers to perform controlled-X and controlled-Z operation.

4. Implementation of Encoders and Decoders for Sparse-Graph Quantum Codes

In this section, we discuss the sparse-graph encoder/decoder implementation in integrated optics based on OHs. Most practical quantum codes belong to the class of dual-containing CSS codes [1], with the (quantum) check matrix represented by

$$\boldsymbol{A} = \left[\begin{array}{c|c} \boldsymbol{H} & \mathbf{0} \\ \mathbf{0} & \boldsymbol{H} \end{array}\right] \tag{13}$$

where $\boldsymbol{H}\boldsymbol{H}^T = 0$, which is equivalent to $C^{\perp}(\boldsymbol{H}) \subset C(\boldsymbol{H})$, where $C(\boldsymbol{H})$ is the code having $\boldsymbol{H}$ as the parity-check matrix, and $C^{\perp}(\boldsymbol{H})$ is its corresponding dual code. The quantum LDPC codes have many advantages over other classes of quantum codes, such as i) the quantum syndrome can be measured with sparse number of interactions, ii) the quasi-cyclic structure of parity-check matrix leads to low decoder complexity compared with random codes, iii) there exist practical decoding algorithms (such as the SPA), and iv) they can be designed to have high quantum code rates. From (13), it follows that by providing that the $\boldsymbol{H}$-matrix of a dual-containing code is sparse, the corresponding $\boldsymbol{A}$-matrix will be sparse as well, while the corresponding stabilizers will require a small number of gates. The main drawback of dual-containing LDPC codes is the fact that they are essentially girth-4 codes, which do not perform well under SPA. On the other hand, it was shown in [5] that entanglement arbitrary classical codes can be used to correct quantum errors and not only girth-4 codes. Because quantum teleportation systems assume the use of entanglement, this approach does not increase the complexity of the system at all. The number of ebits needed in EA LDPC codes is $e = \text{rank}(\boldsymbol{H}\boldsymbol{H}^T)$ (where $\boldsymbol{H}$ is the parity-check matrix of a classical code) so that the minimum number of required EPR pairs is one. For example, a classical code given below has $\text{rank}(\boldsymbol{H}\boldsymbol{H}^T) = 1$ and girth 6

$$\boldsymbol{H} = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

and requires only one ebit to be shared between source and destination.

Since arbitrary classical codes can be used with this approach, including LDPC codes of girth $g \geq 6$, the performance of quantum LDPC codes can significantly be improved. Because two Pauli operators on n-qubits commute if and only if there is an even number of positions in which they differ (neither of which is the identity I operator), we can extend the generators in $\boldsymbol{A}$ (for $\boldsymbol{H}$) by adding e columns ($e = 1$ in example above) so that they can be embedded into a larger Abelian group, which is a procedure known as Abelianization in abstract algebra. In previous paragraphs, we have already shown how to implement the Pauli gates in integrated optics. Therefore, an arbitrary quantum LDPC encoder and decoder can be implemented in integrated optics based on OHs.

5. EA Quantum Sparse-Graph Codes From BIBDs of Unitary Index

In this section, we provide several quite general BIBD-based LDPC code designs with $\text{rank}(\boldsymbol{H}\boldsymbol{H}^T) = 1$ and a girth of 6.

5.1.1. Definition 1

A BIBD(v, k, λ) [4], [12], [13] is a collection of subsets (blocks) of a set V of size v, with a size of each block being k, so that i) each pair of elements occurs in *exactly* λ of the subsets, and ii) every element occurs in exactly $r = \lambda(v-1)/(k-1)$ subsets.

The incidence matrix of a BIBD(v, k, λ) with b blocks, which corresponds to a parity-check matrix of an LDPC code, is a $b \times v$ matrix $\boldsymbol{H} = (h_{ij})$ defined by $h_{ij} = 1$ if the ith block is contains the jth point; otherwise, $h_{ij} = 0$. The following theorem can be used to design EA codes from BIBDs that require only one ebit to be shared between source and destination.

5.1.2. Theorem 1

Let $\boldsymbol{H}$ be a $b \times v$ parity-check matrix of an LDPC code derived from a BIBD$(v, k, 1)$ of odd r. The rank of $\boldsymbol{H}\boldsymbol{H}^T$ is equal to 1, while the corresponding EA LDPC code of CSS type has the parameters $[v, v-2b+1]$ and requires one ebit to be shared between source and destination.

5.1.2.a. Proof: Because any two rows or columns in $\boldsymbol{H}$ of size $b \times v$ derived from BIBD$(v, k, 1)$ overlap in *exactly* one position, by providing that row weight r is odd, the matrix $\boldsymbol{H}\boldsymbol{H}^T$ is an all-one matrix. The rank of the all-one matrix $\boldsymbol{H}\boldsymbol{H}^T$ is 1. Therefore, LDPC codes from BIBDs of unity index $(\lambda = 1)$ and odd r have $e = \text{rank}(\boldsymbol{H}\boldsymbol{H}^T) = 1$, while the number of required ebits to be shared between source and destination is $e = 1$. If the EA code is put in CSS form given by (13), then the parameters of EA codes will be $[v, v-2b+1]$.

Because the girth of codes derived by employing the Theorem 1 is 6, they can significantly outperform quantum dual-containing LDPC codes. Notice that certain blocks in so-called λ-configurations [12] have the overleap of zero and, therefore, cannot be used to design EA codes with $e = 1$. Shrikhande [13] has shown that the generalized Hadamard matrices, affine resolvable BIBDs, group-divisible designs, and orthogonal arrays of strength 2 are all related, and because of these combinatorial objects $\lambda = 0$ or 1, they are not suitable for the design of EA codes of $e = 1$. Notice that if the quantum check matrix is put into the format $\boldsymbol{A} = [\boldsymbol{H}|\boldsymbol{H}]$, then the corresponding EA code has parameters $[v, v-b+1]$. This design can be generalized by employing two BIBDs having the same parameter v, as explained in Theorem 2 below.

5.1.3. Theorem 2

Let $\boldsymbol{H}_1$ be a $b_1 \times v$ parity-check matrix of an LDPC code derived from a BIBD$(v, k_1, 1)$ of odd r_1 and $\boldsymbol{H}_2$ be a $b_2 \times v$ parity-check matrix of an LDPC code derived from a BIBD$(v, k_2, 1)$ of odd r_2. The number of ebits required in corresponding EA code with quantum check matrix $\boldsymbol{A} = [\boldsymbol{H}_1|\boldsymbol{H}_2]$ is $e = \text{rank}(\boldsymbol{H}_1\boldsymbol{H}_2^T + \boldsymbol{H}_2\boldsymbol{H}_1^T)/2 = 1$, while the corresponding EA LDPC code has the parameters $[v, v-b+1]$.

The proof of this theorem is a straightforward generalization of the proof of Theorem 1. Below, we describe three designs belonging to the class of codes from Theorem 1.

5.1.4. Design 1 (Steiner triple system)

If $6t+1$ is a prime power and θ is a primitive root of GF$(6t+1)$, then the t initial blocks $(\theta^i, \theta^{2t+i}, \theta^{4t+i})$ $(i = 0, 1, \ldots, t-1)$ form BIBD$(6t+1, 3, 1)$ with $r = 3t$. The BIBD is formed by adding the elements from GF$(6t+1)$ to the initial blocks. The corresponding LDPC code has rank$(\boldsymbol{H}\boldsymbol{H}^T) = 1$ and a girth of 6. The parity-check matrix used in the example in Section 4 is obtained from Design 1 for $t = 1$.

5.1.5. Design 2 (projective planes)

A finite projective plane of order n, say PG$(2, n)$, is an $(n^2+n+1, n+1, 1)$ BIBD, and $n \geq 2$ and n is a power of prime [12]. The point set of the design consists of all the *points* on PG$(2, n)$, and the block set of the design consist of all *lines* on PG$(2, n)$. The points and lines of a finite projective plane satisfy the following set of axioms: i) Every line consists of the same number of points; ii) any

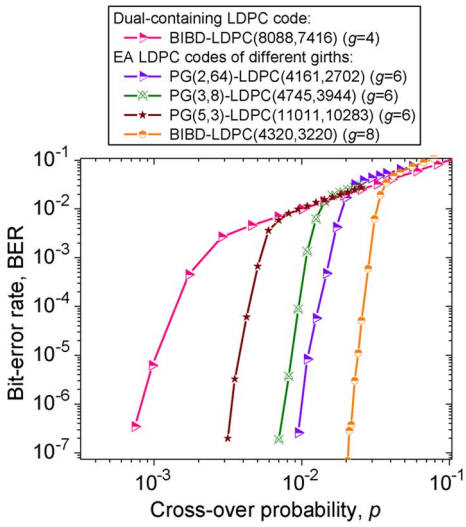


Fig. 6. Sparse-graph quantum codes performance.

two points on the plane are connected by a unique line; iii) any two lines on the plane intersect at a unique point; and iv) a fixed number of lines pass through any point on the plane. Since any two lines on a projective plane intersect at a unique point, there are no parallel lines on the plane $(\lambda = 1)$. The incidence matrix (parity-check matrix of corresponding LDPC codes) of such a design, for $n = 2^s$, is cyclic, and hence, any row of the matrix can be obtained by shifting (right or left) another row of the matrix. Since the row weight $n + 1 = 2^s + 1$ is odd, the corresponding LDPC code has rank$(\boldsymbol{H}\boldsymbol{H}^T) = 1$. The minimum distance of codes from projective planes, affine planes, oval designs, and unitals [14] is at least $2^s + 2$, $2^s + 1$, $2^{s-1} + 1$, and $2^{s/2} + 2$, respectively. Notice, however, that affine-plane-based codes have rank$(\boldsymbol{H}\boldsymbol{H}^T) > 1$, because they contain parallel lines.

5.1.6. Design 3 (m-dimensional projective geometries)

The finite projective geometries [12] PG(m, p^s) are constructed using $(m+1)$-tuples $x = (x_0, x_1, \ldots, x_m)$ of elements x_i from GF(p^s) (p-a prime, s-positive integer), which are not all simultaneously equal to zero, called *points*. Two $(m+1)$-tuples $\boldsymbol{x}$ and $y = (y_0, y_1, \ldots, y_m)$ represent the same point if $\boldsymbol{y} = \lambda \boldsymbol{x}$, where λ is a non-zero element from GF(p^s). Therefore, each point can be represented $p^s - 1$ ways (an equivalence class). The number of points in PG(m, p^s) is $v = [p^{(m+1)s} - 1]/(p^s - 1)$. The points (equivalence classes) can be represented by $[\alpha^i] = \{\alpha^i, \beta\alpha^i, \ldots, \beta^{p^s-2}\alpha^i\}$ $(0 \le i \le v)$, where $\beta = \alpha^v$. Let $[\alpha^i]$ and $[\alpha^j]$ be two distinct points in PG(m, p^s); then, the line passing through them consists of points of the form $[\lambda_1\alpha^i + \lambda_2\alpha^j]$, where $\lambda_1, \lambda_2 \in$ GF(p^s). Because $[\lambda_1\alpha^i + \lambda_2\alpha^j]$ and $[\beta^k\lambda_1\alpha^i + \beta^k\lambda_2\alpha^j]$ represent the same point, each line in PG(m, p^s) consists of $k = (p^{ms} - 1)/(p^s - 1)$ points. The number of lines intersecting at a given point is given by k, and the number of lines in m-dimensional PG is $b = [p^{s(m+1)} - 1](p^{sm} - 1)/[(p^{2s} - 1)(p^s - 1)]$. The parity-check matrix is obtained as the incidence matrix $\boldsymbol{H} = (h_{ij})_{b\times v}$ with rows corresponding to the lines and columns to the points and columns being arranged in the following order: $[\alpha^0], \ldots, [\alpha^\nu]$. $h_{ij} = 1$ if the jth point belongs to ith line, and zero otherwise. Each row has weight $p^s + 1$, and each column has the weight k. Any two rows or columns have exactly one "1" in common, and providing that p^s is even, then the row weight $(p^s + 1)$ will be odd, and the corresponding LDPC code will have rank$(\boldsymbol{H}\boldsymbol{H}^T) = 1$. By defining a parity-check matrix as an incidence matrix with lines corresponding to columns and points to rows, the corresponding LDPC code will have rank$(\boldsymbol{H}\boldsymbol{H}^T) = 1$ by providing that a row weight k is odd.

In Fig. 6, we provide comparison of EA LDPC codes of girth $g = 6$ and 8 against a dual-containing LDPC code. We see that EA LDPC codes outperform, for more than order in magnitude, the corresponding dual-containing LDPC code. The sparse-graph codes of girth $g \ge 8$ have

rank($\boldsymbol{HH}^T$) $= e > 1$ and require e ebits to be shared between source and destination. These codes outperform BIBD-based EA codes of girth 6, as shown in Fig. 5, but have higher decoder complexity.

6. Conclusion

We have shown that different sets of universal quantum gates can be implemented in integrated optics based on OHs/MZIs/DCs and either HNLF or a tap coupler with an APD. We have also shown how to implement Pauli operators (required in QECC) in integrated optics using the same technology. The implementation of the Bell states preparation circuit, which is required in quantum teleportation, in integrated optics has been described as well. To extend the transmission distance of quantum teleportation systems, we proposed an integrated optics circuit that can serve as the photonic quantum relay. Because the QIP relies on delicate superposition states and quantum gates are imperfect, the use of QECC is essential. We have shown that the encoders and decoders for an arbitrary quantum error-correcting code can be implemented based on OHs/MZIs/DCs and HNLFs (or tap couplers with APDs). We have performed Monte Carlo simulations and shown that that the EA sparse-graph codes can significantly outperform corresponding dual-containing LDPC codes. We also provide two theorems that are suitable for the design of EA LDPC codes from BIBDs, which require only one ebit to be shared between the source and the destination. Finally, we provide three BIBD-based EA sparse-graph code constructions.

References

[1] M. A. Neilsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge, U.K.: Cambridge Univ. Press, 2000.

[2] D. J. C. MacKay, G. Mitchison, and P. L. McFadden, "Sparse-graph codes for quantum error correction," *IEEE Trans. Inf. Theory*, vol. 50, no. 10, pp. 2315–2330, Oct. 2004.

[3] I. Djordjevic, "Photonic quantum dual-containing LDPC encoders and decoders," *IEEE Photon. Technol. Lett.*, vol. 21, no. 13, pp. 842–844, Jul. 2009.

[4] I. B. Djordjevic, "Quantum LDPC codes from balanced incomplete block designs," *IEEE Commun. Lett.*, vol. 12, no. 5, pp. 389–391, May 2008.

[5] T. Brun, I. Devetak, and M.-H. Hsieh, "Correcting quantum errors with entanglement," *Science*, vol. 314, no. 5798, pp. 436–439, Oct. 2006.

[6] T. C. Ralph, N. K. Langford, T. B. Bell, and A. G. White, "Linear optical controlled-NOT gate in the coincidence basis," *Phys. Rev. A, Gen. Phys.*, vol. 65, no. 6, pp. 062324-1–062324-5, Jun. 2002.

[7] A. Politi, M. Cryan, J. Rarity, S. Yu, and J. L. O'Brien, "Silica-on-silicon waveguide quantum circuits," *Science*, vol. 320, no. 5876, pp. 646–649, May 2008.

[8] A. Barenco, "A universal two-bit quantum computation," in *Proc. R. Soc. Lond. A, Math. Phys. Sci.*, Jun. 1995, vol. 449, no. 1937, pp. 679–683.

[9] D. Deutsch, "Quantum computational networks," in *Proc. R. Soc. Lond. A, Math. Phys. Sci.*, Sep. 1989, vol. 425, no. 1868, pp. 73–90.

[10] S. Radic and C. J. McKinistrie, "Optical amplification and signal processing in highly nonlinear optical fiber," *IEICE Trans. Electron.*, vol. E88-C, no. 5, pp. 859–869, May 2005.

[11] S.-T. Cheng, C.-Y. Wang, and M.-H. Tao, "Quantum communication for wireless wide-area networks," *IEEE J. Sel. Areas Commun.*, vol. 23, no. 7, pp. 1424–1432, Jul. 2005.

[12] D. Raghavarao, *Constructions and Combinatorial Problems in Design of Experiments*. New York: Dover, 1988.

[13] S. S. Shrikhande, "Generalized Hadamard matrices and orthogonal arrays of strength two," *Can. J. Math.*, vol. 16, pp. 736–740, 1964.

[14] I. Djordjevic, S. Sankaranarayanan, and B. Vasic, "Projective-plane iteratively decodable block codes for WDM high-speed long-haul transmission systems," *J. Lightw. Technol.*, vol. 22, no. 3, pp. 695–702, Mar. 2004.